PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-110211
(43)Date of publication of application : 23.04.1999

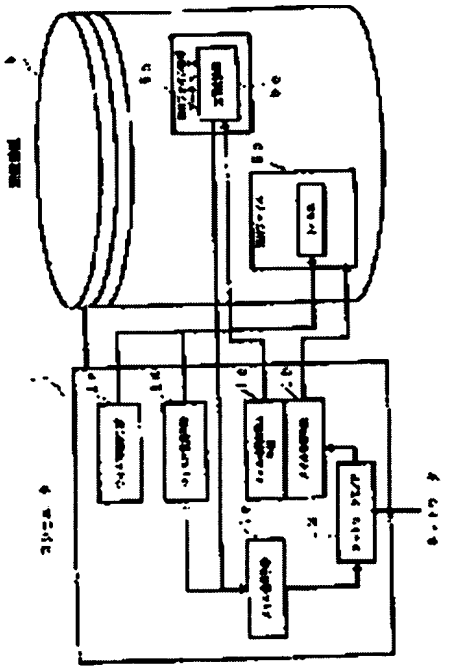
(51)Int.Cl. G06F 9/06
G06F 13/00

(21)Application number : 09-266426
(22)Date of filing : 30.09.1997

(71)Applicant : BROTHER IND LTD
(72)Inventor : FUJII NORIHISA

(54) COMPUTER SYSTEM, COMPUTER VIRUS OPPOSITION METHOD AND STORAGE MEDIUM FOR RECORDING COMPUTER VIRUS OPPOSITION PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a counter-measure against a computer virus in a computer system connected to a network.
SOLUTION: An electronic mail including an accompanying file from other computer on a network is received by a mail reception means 1b and, at the same time, a transmitter is detected by a mail transmitter detection means 1c and stored in a storage device 5 as transmitter information 5c of an accompanying file 5a and of an information database 5b. Then, when a virus is detected by a virus detection means 1d, a virus extermination means 1e exterminates the virus, and virus detection information is attached by a virus extermination software by the main transmission means 1a and transmitted to the transmitter.



LEGAL STATUS

[Date of request for examination] 07.08.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－110211

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	13/00	３５１		13/00	３５１Ｇ

審査請求　未請求　請求項の数12　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－266426

(22)出願日　平成９年(1997)９月30日

(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番１号

(72)発明者　藤井　則久
愛知県名古屋市瑞穂区苗代町15番１号　ブラザー工業株式会社内

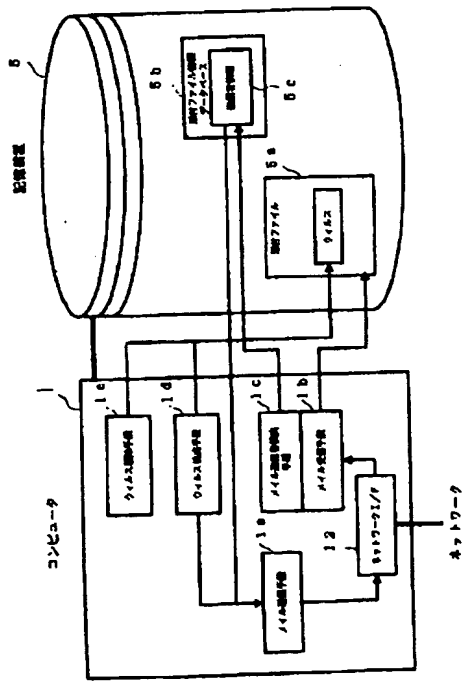
(74)代理人　弁理士　石川　泰男　（外２名）

(54)【発明の名称】　コンピュータシステム及びコンピュータウィルス対抗方法並びにコンピュータウィルス対抗プログラムが記録された記録媒体

(57)【要約】

【課題】　ネットワークに接続されたコンピュータシステムにおけるコンピュータウィルスに対する対抗方法を提供する。

【解決手段】　ネットワーク上の他のコンピュータからの添付ファイルを含む電子メールをメイル受信手段１ｂにより受信するとともに、メイル送信者検出手段１ｃにより送信元を検出して、記憶装置４に添付ファイル４ａ及び情報データベース４ｂの送信者情報４ｃとして記憶する。そして、ウィルス検出手段１ｄによりウィルスが検出されると、ウィルス駆除手段１ｅがウィルスを駆除し、メイル送信手段１ａによりウィルス検出情報をウィルス駆除ソフトウェアを添付して送信元に対し送信する。



【特許請求の範囲】
【請求項１】　複数のコンピュータがネットワークにより相互接続されたコンピュータシステムであって、
前記ネットワークを介して他のコンピュータからファイルを受信する受信手段と、
前記受信手段によりファイルを受信する際、当該受信ファイルの送信元であるコンピュータを判別する判別手段と、
前記受信ファイルにおけるコンピュータウィルスの存在を検出する検出手段と、
前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記送信元であるコンピュータに前記コンピュータウィルスの検出情報を送信する送信手段と、
を備えることを特徴とするコンピュータシステム。
【請求項２】　前記判別手段により判別された前記送信元であるコンピュータを前記受信ファイルと関係付けて示すファイル付属情報を記憶する記憶手段を更に備えるとともに、
前記送信手段は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記ファイル付属情報により示される前記受信ファイルの前記送信元であるコンピュータに、前記コンピュータウィルスの検出情報を送信することを特徴とする請求項１に記載のコンピュータシステム。
【請求項３】　前記記憶手段に前記ファイル付属情報が記憶された受信ファイルを前記ネットワークを介して更に別のコンピュータに転送する転送手段と、
前記コンピュータウィルスの検出情報を受信する検出情報受信手段とを更に備え、
前記送信手段は、前記転送手段により転送したファイルに関して前記検出情報受信手段が前記コンピュータウィルスの検出情報を受信した場合、当該ファイルに関して前記記憶手段から前記ファイル付属情報を検出し、当該ファイル付属情報が示すファイルの送信元に前記コンピュータウィルスの検出情報を送信することを特徴とする請求項２に記載のコンピュータシステム。
【請求項４】　前記送信手段は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、検出された前記コンピュータウィルスを駆除するコンピュータウィルス駆除ソフトウェアを更に送信することを特徴とする請求項１から請求項３に記載のコンピュータシステム。
【請求項５】　複数のコンピュータがネットワークにより相互接続されたコンピュータシステムにおけるコンピュータウィルス対抗方法であって、
前記ネットワークを介して他のコンピュータからファイルを受信する受信工程と、
前記受信工程によりファイルを受信する際、当該受信ファイルの送信元であるコンピュータを判別する判別工程と、
前記受信ファイルにおけるコンピュータウィルスの存在を検出する検出工程と、
前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記送信元であるコンピュータに前記コンピュータウィルスの検出情報を送信する送信工程と、
を備えることを特徴とするコンピュータウィルス対抗方法。
【請求項６】　前記判別工程により判別された前記送信元であるコンピュータを前記受信ファイルと関係付けて示すファイル付属情報を記憶する記憶工程を更に備えるとともに、
前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記ファイル付属情報により示される前記受信ファイルの前記送信元であるコンピュータに、前記コンピュータウィルスの検出情報を送信することを特徴とする請求項５に記載のコンピュータウィルス対抗方法。
【請求項７】　前記記憶工程にて前記ファイル付属情報が記憶された受信ファイルを前記ネットワークを介して更に別のコンピュータに転送する転送工程と、
前記コンピュータウィルスの検出情報を受信する検出情報受信工程とを更に備え、
前記送信工程は、前記転送工程により転送したファイルに関して前記検出情報受信工程が前記コンピュータウィルスの検出情報を受信した場合、当該ファイルに関して前記記憶工程により記憶された前記ファイル付属情報を検出し、当該ファイル付属情報が示すファイルの送信元に前記コンピュータウィルスの検出情報を送信することを特徴とする請求項６に記載のコンピュータウィルス対抗方法。
【請求項８】　前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、検出された前記コンピュータウィルスを駆除するコンピュータウィルス駆除ソフトウェアを更に送信することを特徴とする請求項５から請求項７に記載のコンピュータウィルス対抗方法。
【請求項９】　複数のコンピュータがネットワークにより相互接続されたコンピュータシステムに含まれるコンピュータに、
前記ネットワークを介して他のコンピュータからファイルを受信する受信工程と、
前記受信工程によりファイルを受信する際、当該受信ファイルの送信元であるコンピュータを判別する判別工程と、
前記受信ファイルにおけるコンピュータウィルスの存在を検出する検出工程と、
前記受信ファイルにおいて前記コンピュータウィルスの

存在が検出された場合、前記ネットワークを介して前記送信元であるコンピュータに前記コンピュータウィルスの検出情報を送信する送信工程と、
を実行させることを特徴とするコンピュータウィルス対抗プログラムが記録された記録媒体。
【請求項１０】　前記判別工程により判別された前記送信元であるコンピュータを前記受信ファイルと関係付けて示すファイル付属情報を記憶する記憶工程を更に実行させるとともに、
前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記ファイル付属情報により示される前記受信ファイルの前記送信元であるコンピュータに、前記コンピュータウィルスの検出情報を送信することを特徴とする請求項９に記載のコンピュータウィルス対抗プログラムが記録された記録媒体。
【請求項１１】　前記記憶工程にて前記ファイル付属情報が記憶された受信ファイルを前記ネットワークを介して更に別のコンピュータに転送する転送工程と、
前記コンピュータウィルスの検出情報を受信する検出情報受信工程とを更に備え、
前記送信工程は、前記転送工程により転送したファイルに関して前記検出情報受信工程が前記コンピュータウィルスの検出情報を受信した場合、当該ファイルに関して前記記憶工程により記憶された前記ファイル付属情報を検出し、当該ファイル付属情報が示すファイルの送信元に前記コンピュータウィルスの検出情報を送信することを特徴とする請求項１０に記載のコンピュータウィルス対抗プログラムが記録された記録媒体。
【請求項１２】　前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、検出された前記コンピュータウィルスを駆除するコンピュータウィルス駆除ソフトウェアを更に送信することを特徴とする請求項９から請求項１１に記載のコンピュータウィルス対抗プログラムが記録された記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークにより相互に接続された複数のコンピュータがネットワークを経由してファイルを送受信するに際し、コンピュータウィルスの攻撃を防御するためのコンピュータシステム及びコンピュータウィルス対抗方法並びにコンピュータウィルス対抗プログラムを記録した記録媒体の技術分野に属する。
【０００２】
【従来の技術】従来から、不特定多数の人間が利用可能なコンピュータシステムにおける人為的要因によるトラブルとして、コンピュータウィルスの問題がある。コンピュータウィルスは生物ウィルスと同様、自己増殖能力があり、他のプログラム等に感染しつつ、システムの動作を異常にしたり、データを破壊したりするなどコンピュータシステムに攻撃を加え、被害を拡大していく。
【０００３】一方、今日のコンピュータシステムは多数のコンピュータがネットワークにより相互に接続され、電子メール等を利用して互いにデータの送受信を行う。そして、フロッピーディスク等の物理的媒体による感染経路と比べ、ネットワークによってコンピュータウィルスが媒介される場合、急速かつ大規模に感染するため被害規模は一層大きくなる。よって、コンピュータシステムのセキュリティ維持のため、コンピュータウィルスを駆除するワクチンソフトウェア等による何らかの対策を施し、コンピュータウィルスからの攻撃を防ぐことが重要となる。
【０００４】
【発明が解決しようとする課題】しかしながら、コンピュータシステムのオープン化、パーソナル化に伴い、セキュリティレベルの低いコンピュータ端末のネットワークへの接続を排除することは容易ではなく、上述のワクチンソフトウェア等によるコンピュータウィルスに対する対策をネットワークに接続可能な全てのコンピュータ端末に導入することは困難である。そのため、コンピュータウィルスに対する対策が不十分なコンピュータ端末を同一の感染源としてウィルス感染を繰り返し、コンピュータシステム全体に被害を広げるおそれがある。
【０００５】また、ネットワークを経由して複雑な経路を経てコンピュータウィルスに感染したファイルが伝搬された後、コンピュータウィルスが発見され、発見されたコンピュータ端末においてワクチンソフトウェア等による対策を施すことができる場合であっても、ファイルには感染経路を判別する情報は付与されてないため、、別の感染経路を経てコンピュータウィルスが伝搬することを防止できない。
【０００６】以上にように、従来、ネットワークを用いるコンピュータシステムにおいては、コンピュータウィルスによる被害を防ぎ、安全なコンピュータシステムの運用を図ることが困難である点で問題があった。
【０００７】そこで、本発明は、上記問題点を解決し、ネットワークを経由してコンピュータウィルスの感染が拡大することを防止し、コンピュータウィルスに対する迅速な防御策を講じることができるコンピュータシステム及びコンピュータウィルス対抗方法並びにコンピュータウィルス対抗プログラムが記録された記録媒体を提供することを課題としている。
【０００８】
【課題を解決するための手段】前記課題を解決するために、請求項１に記載のコンピュータシステムは、複数のコンピュータがネットワークにより相互接続されたコンピュータシステムであって、前記ネットワークを介して他のコンピュータからファイルを受信する受信手段と、前記受信手段によりファイルを受信する際、当該受信フ

ファイルの送信元であるコンピュータを判別する判別手段と、前記受信ファイルにおけるコンピュータウィルスの存在を検出する検出手段と、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記送信元であるコンピュータに前記コンピュータウィルスの検出情報を送信する送信手段と、を備えることを特徴とする。

【０００９】請求項１に記載のコンピュータシステムによれば、ネットワークを介して他のコンピュータから受信手段によりファイルを受信する際、受信ファイルの送信元であるコンピュータが判別手段により判別されるとともに、受信ファイルにおけるコンピュータウィルスの有無が検出手段により検出される。そして、コンピュータウィルスが検出されると、送信手段により送信元のコンピュータに対し、ネットワークを介して、コンピュータウィルスの検出情報が送信される。よって、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識でき、コンピュータウィルスに対する適切な対策を施すことが可能となる。

【００１０】請求項２に記載のコンピュータシステムは、請求項１に記載のコンピュータシステムにおいて、前記判別手段により判別された前記送信元であるコンピュータを前記受信ファイルと関係付けて示すファイル付属情報を記憶する記憶手段を更に備えるとともに、前記送信手段は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記ファイル付属情報により示される前記受信ファイルの前記送信元であるコンピュータに、前記コンピュータウィルスの検出情報を送信することを特徴とする。

【００１１】請求項２に記載のコンピュータシステムによれば、判別手段により判別されたファイルの送信元であるコンピュータを示すファイル付属情報を、受信ファイルと関係付けて記憶手段に記憶する。その後、受信ファイルにおいてコンピュータウィルスが検出手段により検出された場合、送信元であるコンピュータがファイル付属情報として記憶してあれば、送信手段により送信元のコンピュータに対し、ネットワークを介して、コンピュータウィルスの検出情報が送信される。よって、送信元のコンピュータが、ファイル送信直後にコンピュータウィルスを検出できなくても、ファイルの受信履歴としてファイル付属情報が付与されるので、後にコンピュータウィルスを発見した場合でもファイル送信元を判別でき、請求項１の場合と同様、コンピュータウィルスの感染を認識でき、適切な対策を施すことが可能となる。

【００１２】請求項３に記載のコンピュータシステムは、請求項２に記載のコンピュータシステムにおいて、前記記憶手段に前記ファイル付属情報が記憶された受信ファイルを前記ネットワークを介して更に別のコンピュータに転送する転送手段と、前記コンピュータウィルスの検出情報を受信する検出情報受信手段とを更に備え、前記送信手段は、前記転送手段により転送したファイルに関して前記検出情報受信手段が前記コンピュータウィルスの検出情報を受信した場合、当該ファイルに関して前記記憶手段から前記ファイル付属情報を検出し、当該ファイル付属情報が示すファイルの送信元に前記コンピュータウィルスの検出情報を送信することを特徴とする。

【００１３】請求項３に記載のコンピュータシステムによれば、受信した受信ファイルを、転送手段により、ネットワークを介して更に別のコンピュータに転送する。その後、検出情報受信手段により転送したファイルに関するコンピュータウィルスの検出情報を受信した場合、転送したファイルに関するファイル付属情報を記憶手段から検出し、ファイル付属情報が示すファイルの送信元に対し、受信したコンピュータウィルスの検出情報を更に送信する。よって、受信ファイルのコンピュータウィルスを発見できないまま、別のコンピュータにそのファイルを転送した場合でも、後に別のコンピュータから送信される情報によりそのファイルがコンピュータウィルスに感染していることが判明すると、送信元のコンピュータにコンピュータウィルスの存在を知らしめることができ、コンピュータウィルスに対する適切な対策を施すことが可能となる。

【００１４】請求項４に記載のコンピュータシステムは、請求項１から請求項３に記載のコンピュータシステムにおいて、前記送信手段は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、検出された前記コンピュータウィルスを駆除するコンピュータウィルス駆除ソフトウェアを更に送信することを特徴とする。

【００１５】請求項４に記載のコンピュータシステムによれば、受信ファイルにコンピュータウィルスが検出された場合、検出されたコンピュータウィルスを駆除するための駆除ソフトウェアを、送信手段によりファイルの送信元のコンピュータに対し送信する。よって、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識できることに加え、コンピュータウィルスに対する対策手段を併せて入手できることとなり、速やかに適切な対策を施すことが可能となる。

【００１６】請求項５に記載のコンピュータウィルス対抗方法は、複数のコンピュータがネットワークにより相互接続されたコンピュータシステムにおけるコンピュータウィルス対抗方法であって、前記ネットワークを介して他のコンピュータからファイルを受信する受信工程と、前記受信工程によりファイルを受信する際、当該受信ファイルの送信元であるコンピュータを判別する判別工程と、前記受信ファイルにおけるコンピュータウィルスの存在を検出する検出工程と、前記受信ファイルにお

いて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記送信元であるコンピュータに前記コンピュータウィルスの検出情報を送信する送信工程と、を備えることを特徴とする。

【００１７】請求項５に記載のコンピュータウィルス対抗方法によれば、ネットワークを介して他のコンピュータから受信工程によりファイルを受信する際、受信ファイルの送信元であるコンピュータが判別工程により判別されるとともに、受信ファイルにおけるコンピュータウィルスの有無が検出工程により検出される。そして、コンピュータウィルスが検出されると、送信工程により送信元のコンピュータに対し、ネットワークを介して、コンピュータウィルスの検出情報が送信される。よって、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識でき、コンピュータウィルスに対する適切な対策を施すことが可能となる。

【００１８】請求項６に記載のコンピュータウィルス対抗方法は、請求項５に記載のコンピュータウィルス対抗方法において、前記判別工程により判別された前記送信元であるコンピュータを前記受信ファイルと関係付けて示すファイル付属情報を記憶する記憶工程を更に備えるとともに、前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記ファイル付属情報により示される前記受信ファイルの前記送信元であるコンピュータに、前記コンピュータウィルスの検出情報を送信することを特徴とする。

【００１９】請求項６に記載のコンピュータウィルス対抗方法によれば、判別工程により判別されたファイルの送信元であるコンピュータを示すファイル付属情報を、受信ファイルと関係付けて記憶工程により記憶する。その後、受信ファイルにおいてコンピュータウィルスが検出工程により検出された場合、送信元であるコンピュータがファイル付属情報として記憶してあれば、送信工程により送信元のコンピュータに対し、ネットワークを介して、コンピュータウィルスの検出情報が送信される。よって、送信元のコンピュータが、ファイル送信直後にコンピュータウィルスを検出できなくても、ファイルの受信履歴としてファイル付属情報が付与されるので、後にコンピュータウィルスを発見した場合でもファイル送信元を判別でき、請求項５の場合と同様、コンピュータウィルスの感染を認識でき、適切な対策を施すことが可能となる。

【００２０】請求項７に記載のコンピュータウィルス対抗方法は、請求項６に記載のコンピュータウィルス対抗方法において、前記記憶工程により前記ファイル付属情報が記憶された受信ファイルを前記ネットワークを介して更に別のコンピュータに転送する転送工程と、前記コンピュータウィルスの検出情報を受信する検出情報受信工程とを更に備え、前記送信工程は、前記転送工程により転送したファイルに関して前記検出情報受信工程が前記コンピュータウィルスの検出情報を受信した場合、当該ファイルに関して前記記憶工程により記憶された前記ファイル付属情報を検出し、当該ファイル付属情報が示すファイルの送信元に前記コンピュータウィルスの検出情報を送信することを特徴とする。

【００２１】請求項７に記載のコンピュータウィルス対抗方法によれば、受信した受信ファイルを、転送工程により、ネットワークを介して更に別のコンピュータに転送する。その後、検出情報受信工程により転送したファイルに関するコンピュータウィルスの検出情報を受信した場合、転送したファイルに関する記憶工程により記憶されたファイル付属情報を検出し、ファイル付属情報が示すファイルの送信元に対し、受信したコンピュータウィルスの検出情報を更に送信する。よって、受信ファイルのコンピュータウィルスを発見できないまま、別のコンピュータにそのファイルを転送した場合でも、後に別のコンピュータから送信される情報によりそのファイルがコンピュータウィルスに感染していることが判明すると、送信元のコンピュータにコンピュータウィルスの存在を知らしめることができ、コンピュータウィルスに対する適切な対策を施すことが可能となる。

【００２２】請求項８に記載のコンピュータウィルス対抗方法は、請求項５から請求項７に記載のコンピュータウィルス対抗方法において、前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、検出された前記コンピュータウィルスを駆除するコンピュータウィルス駆除ソフトウェアを更に送信することを特徴とする。

【００２３】請求項８に記載のコンピュータウィルス対抗方法によれば、受信ファイルにコンピュータウィルスが検出された場合、検出されたコンピュータウィルスを駆除するための駆除ソフトウェアを、送信工程によりファイルの送信元のコンピュータに対し送信する。よって、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識できることに加え、コンピュータウィルスに対する対策手段を併せて入手できることとなり、速やかに適切な対策を施すことが可能となる。

【００２４】請求項９に記載のコンピュータウィルス対抗プログラムが記録された記録媒体は、複数のコンピュータがネットワークにより相互接続されたコンピュータシステムに含まれるコンピュータに、前記ネットワークを介して他のコンピュータからファイルを受信する受信工程と、前記受信工程によりファイルを受信する際、当該受信ファイルの送信元であるコンピュータを判別する判別工程と、前記受信ファイルにおけるコンピュータウィルスの存在を検出する検出工程と、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された

場合、前記ネットワークを介して前記送信元であるコンピュータに前記コンピュータウィルスの検出情報を送信する送信工程とを実行させることを特徴とする。

【００２５】請求項９に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、ネットワークを介して他のコンピュータから受信工程によりファイルを受信する際、受信ファイルの送信元であるコンピュータが判別工程により判別されるとともに、受信ファイルにおけるコンピュータウィルスの有無が検出工程により検出される。そして、コンピュータウィルスが検出されると、送信工程により送信元のコンピュータに対し、ネットワークを介して、コンピュータウィルスの検出情報が送信される。よって、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識でき、コンピュータウィルスに対する適切な対策を施すことが可能となる。

【００２６】請求項１０に記載のコンピュータウィルス対抗プログラムが記録された記録媒体は、請求項９に記載のコンピュータウィルス対抗プログラムが記録された記録媒体において、前記判別工程により判別された前記送信元であるコンピュータを前記受信ファイルと関係付けて示すファイル付属情報を記憶する記憶工程を更に実行させるとともに、前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、前記ネットワークを介して前記ファイル付属情報により示される前記受信ファイルの前記送信元であるコンピュータに、前記コンピュータウィルスの検出情報を送信することを特徴とする。

【００２７】請求項１０に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、判別工程により判別されたファイルの送信元であるコンピュータを示すファイル付属情報を、受信ファイルと関係付けて記憶工程により記憶する。その後、受信ファイルにおいてコンピュータウィルスが検出工程により検出された場合、送信元であるコンピュータがファイル付属情報として記憶してあれば、送信工程により送信元のコンピュータに対し、ネットワークを介して、コンピュータウィルスの検出情報が送信される。よって、送信元のコンピュータが、ファイル送信直後にコンピュータウィルスを検出できなくても、ファイルの受信履歴としてファイル付属情報が付与されるので、後にコンピュータウィルスを発見した場合でもファイル送信元を判別でき、請求項９の場合と同様、コンピュータウィルスの感染を認識でき、適切な対策を施すことが可能となる。

【００２８】請求項１１に記載のコンピュータウィルス対抗プログラムが記録された記録媒体は、請求項１０に記載のコンピュータウィルス対抗プログラムが記録された記録媒体において、前記記憶工程により記憶された前記ファイル付属情報を前記ネットワークを介して更に別のコンピュータに転送する転送工程と、前記コンピュータウィルスの検出情報を受信する検出情報受信工程とを更に備え、前記送信工程は、前記転送工程により転送したファイルに関して前記検出情報受信工程が前記コンピュータウィルスの検出情報を受信した場合、当該ファイルに関して前記記憶工程により記憶された前記ファイル付属情報を検出し、当該ファイル付属情報が示すファイルの送信元に前記コンピュータウィルスの検出情報を送信することを特徴とする。

【００２９】請求項１１に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、受信した受信ファイルを、転送工程により、ネットワークを介して更に別のコンピュータに転送する。その後、検出情報受信工程により転送したファイルに関するコンピュータウィルスの検出情報を受信した場合、記憶工程により記憶された転送したファイルに関するフィイル付属情報を検出し、ファイル付属情報が示すファイルの送信元に対し、受信したコンピュータウィルスの検出情報を更に送信する。よって、受信ファイルのコンピュータウィルスを発見できないまま、別のコンピュータにそのファイルを転送した場合でも、後に別のコンピュータから送信される情報によりそのファイルがコンピュータウィルスに感染していることが判明すると、送信元のコンピュータにコンピュータウィルスの存在を知らしめることができ、コンピュータウィルスに対する適切な対策を施すことが可能となる。

【００３０】請求項１２に記載のコンピュータウィルス対抗プログラムが記録された記録媒体は、請求項９から請求項１１に記載のコンピュータウィルス対抗プログラムが記録された記録媒体において、前記送信工程は、前記受信ファイルにおいて前記コンピュータウィルスの存在が検出された場合、検出された前記コンピュータウィルスを駆除するコンピュータウィルス駆除ソフトウェアを更に送信することを特徴とする。

【００３１】請求項１２に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、受信ファイルにコンピュータウィルスが検出された場合、検出されたコンピュータウィルスを駆除するための駆除ソフトウェアを、送信工程によりファイルの送信元のコンピュータに対し送信する。よって、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識できることに加え、コンピュータウィルスに対する対策手段を併せて入手できることとなり、速やかに適切な対策を施すことが可能となる。

【００３２】

【発明の実施の形態】以下、本発明の一実施形態を図面に基づいて説明する。

【００３３】始めに、図１に示すブロック図により、本

実施形態に係るコンピュータシステムの概略構成を説明する。

【００３４】図１に示すように、本実施形態のコンピュータシステムは、コンピュータ１、２、３と、それらを接続するネットワーク４とを備えている。そして、コンピュータ１から出力されるデータはネットワーク４を経由してコンピュータ２又は、コンピュータ３へ送信され、コンピュータ２又はコンピュータ３から出力されるデータはネットワーク４を経由してコンピュータ１へ送信される。

【００３５】本実施形態においては、コンピュータ１、２、３が、データ送受信手段として電子メールを利用する場合について説明する。コンピュータ１、２、３は、ネットワークを経由して電子メールを送受信することにより、テキストデータの送受信に加え、コード化された実行ファイルを電子メールの添付ファイルとして送受信することができる。なお、コンピュータ２、３はコンピュータ１と同じ構成の装置であり、コンピュータ２、３については説明を省略する。

【００３６】次に、図２に示すブロック図により、本実施形態に係るコンピュータ１のハードウェアの構成を説明する。

【００３７】コンピュータ１は、図２に示すように、ＣＰＵ１０と、コンピュータ１における処理に必要なデータを入力するための入力部１１と、ネットワークインターフェース１２と、ＲＯＭ１３と、ＲＡＭ１４と、ディスプレイ１５と、記憶装置用インターフェース１６と、これらの各構成要素を接続するバス１７とを備えている。

【００３８】ネットワークインターフェース１２は、コンピュータ１から出力するデータ及びコンピュータ１に入力するデータに対してプロトコルの変換等を行い、ネットワーク４を経由したコンピュータ１によるデータの送受信を可能としている。

【００３９】入力部１１は、キーボード、マウス等よりなり、コンピュータ１の使用者の操作により入力されたデータを、バス１７を介してＣＰＵ１０等に出力する。

【００４０】ＲＯＭ１３は、ＣＰＵ１０における処理に必要な制御用のプログラムを記憶している読み出し専用のメモリであり、所定のタイミングで必要なプログラムを読み出して、バス１７に出力する。

【００４１】ＲＡＭ１４は、ＣＰＵ１０が実行する各種プログラムを保持するとともに、ＣＰＵ１０における処理に必要なデータ等を一時的に記憶し、必要に応じてバス１７に出力する。

【００４２】ディスプレイ１５は、ＣＰＵ１０における処理に必要な表示を行う。

【００４３】記憶装置用インターフェース１６は、ファイル受信の際、ファイル及びファイル付属情報等を格納する記憶手段としての記憶装置５に対するインターフェース動作を行う。

【００４４】ＣＰＵ１０は、ＲＡＭ１４に記憶されているプログラムに基づいて、自ら演算処理等を行い、あるいは上述した各構成要素を制御し、コンピュータ１を後述する各手段として機能させる。

【００４５】次に、図３に示すブロック図により、本実施形態に係るコンピュータ１を機能の面からとらえて説明する。

【００４６】ここで、図３においては、コンピュータ１とコンピュータ２のファイルやメッセージ等のデータ送受信手段として、ネットワーク４を介した電子メールを利用する場合について説明する。

【００４７】図３に示すように、本実施形態における機能は、コンピュータ１におけるメイル送信手段１ａ、メイル受信手段１ｂ、メイル送信者検出手段１ｃ、ウィルス検出手段１ｄ、ウィルス駆除手段１ｅを含む。なお、これら各手段は実際にはコンピュータ１のＲＯＭ１３に記憶され、あるいはＲＡＭ１４に展開されるプログラムをＣＰＵ１０が実行することにより実現される。また、コンピュータ１に接続される記憶装置５に保存すべき情報の格納領域として、添付ファイル領域５ａ、添付ファイル情報データベース領域５ｂがあり、添付ファイル情報データベース領域５ｂには、さらに送信者情報領域５ｃが含まれる。

【００４８】メイル送信手段１ａは、ネットワーク４を経由して、所定のアドレスで示される他のコンピュータに対し、ネットワークインターフェース１２を介して所定のフォーマットによる電子メールを送信する手段である。この電子メールには、テキストデータに加え、実行ファイル等の添付ファイルをコード化して含めることができる。そして、ウィルス検出情報やワクチンソフトウェア等を添付ファイルとして含む電子メールが、後述する処理に従いメイル送信手段１ａにより送信される。

【００４９】メイル受信手段１ｂは、ネットワーク４を経由して、他のコンピュータから、ネットワークインターフェース１２を介して前述の電子メールを受信する手段である。この場合も電子メールには、テキストデータに加え、実行ファイル等の添付ファイルをコード化して含めることができる。さらに、メイル受信手段１ｂにより添付ファイルとして実行ファイルを含む電子メールを受信すると、これをデコードして実行ファイルを抽出し、記憶装置５における添付ファイル領域５ａに保存する。

【００５０】メイル送信者検出手段１ｃは、前述した電子メールのデコードを行う際に、電子メールのヘッダ部分を参照し、電子メールの送信元のアドレス情報を判別し、添付された受信ファイルの送信元であるコンピュータを特定する手段である。特定された電子メールの送信者を示すデータは、記憶装置５における送信者情報領域５ｃに保存される。そして、後にコンピュータウィルス

情報を他のコンピュータから受信した場合、過去にコンピュータウィルスが検出されたファイルを受信した履歴が、この送信者情報領域５ｃを参照することにより判断することができる。

【００５１】なお、この送信者情報領域５ｃは、メイル受信手段１ｂがファイル受信の際にのみ受信した電子メールの送信元を判別する場合には、設けない構成とすることもできる。この場合には、過去のファイル受信履歴に基づく受信ファイルの送信元の特定は行われない。

【００５２】ウィルス検出手段１ｄは、記憶装置５の添付ファイル領域５ａの各添付ファイルがコンピュータウィルスに感染しているかどうかを検出する手段である。コンピュータウィルスの検出するには様々な方法があるが、静的な検出方法と動的な検出方法とに大別できる。

【００５３】静的ウィルス検出方法は、既知のコンピュータウィルスに関するデータベースに基づき、対象ファイル内部とシステム領域を、起動時、終了時、一定時刻等の所定のタイミングで検索し、コンピュータウィルスの存在を調べる方法である。コンピュータウィルスは、新しいタイプのものが頻繁に出現するため、前記データベースの内容は適宜更新する必要がある。

【００５４】動的ウィルス検出方法は、コンピュータウィルスが、自らを複製するため行う実行ファイルやシステム領域の変更などの一定の動作を監視し、コンピュータウィルを検出する方法である。コンピュータウィルスに関するデータベースを設けなくても、未知のコンピュータウィルスを検出できる点でメリットを有する。

【００５５】ウィルス駆除手段１ｅは、コンピュータウィルスに感染したファイルからコンピュータウィルスを除去するための手段であり、複数のコンピュータウィルスの種類に対応したワクチンソフトウェアが用意される。そして、発見されたコンピュータウィルスを駆除するのに最適なワクチンソフトウェアを、後述する処理に従い、ネットワーク４を介して他のコンピュータに送信することができる。

【００５６】なお、図３においては、本実施形態のデータ送受信手段として、電子メールを用いた場合について説明したが、本実施形態はこれに限定されるものでなく、その他様々なデータ通信手段により実現することができる。また、既存のデータ通信手段を用いる場合に限られず、コンピュータウィルス情報等の送受信に適する専用のデータ送受信手段を構築することも可能である。

【００５７】次に、図４及び図５に示すフローチャートにより、本実施形態に係るコンピュータシステムのコンピュータウィルスに対する防御方法を説明する。

【００５８】図４に、コンピュータ１がコンピュータ２から添付ファイルを含む電子メールを受信した場合に、コンピュータ１において行われる処理のフローチャートを示す。

【００５９】図４に示すように、コンピュータ１において添付ファイルを含む電子メールがメイル受信手段１ｂにより受信されると、まず、受信した電子メールの実行ファイル等の添付ファイルがデコードされ、記憶装置５の添付ファイル領域５ａに保存する（ステップＳ１）。そして、メイル送信者検出手段１ｃが検出した電子メールの送信元であるコンピュータ２を示すアドレス情報を記憶装置５の添付ファイル情報データベース領域５ｂに付随する送信者情報領域５ｃに登録する（ステップＳ２）。

【００６０】次いで、ウィルス検出手段１ｄにより添付ファイル領域５ａにおけるコンピュータウィルスの有無を前述の方法により判別する（ステップＳ３）。その結果、コンピュータウィルスを検出した場合（ステップＳ３；ＹＥＳ）、ウィルス駆除手段１ｅが最適なワクチンソフトウェアを用いてコンピュータウィルスを取り除く（ステップＳ４）。さらに、このワクチンソフトウェアはウィルス通知メールに添付されて、送信者情報領域５ｃの該当情報が示す受信した電子メールの送信元であるコンピュータ２に対して、メイル送信手段１ａにより送信され（ステップＳ５）、処理が終了する。このウィルス通知メールには、コンピュータウィルスを発見した旨のメッセージ、発見したコンピュータウィルスの名称、及び受信したファイル名などがテキスト情報として記述されるとともに、前記ワクチンソフトウェア及びコンピュータウィルスが発見されたファイルを添付ファイルとして含む。

【００６１】一方、コンピュータウィルスが検出されない場合（ステップＳ３；ＮＯ）、ステップＳ４とステップＳ５の処理を行わず、処理を終了する。

【００６２】以上の処理により、コンピュータウィルスの伝搬元である電子メールの送信者は、コンピュータウィルスに関する情報と駆除に必要なワクチンソフトウェアを入手することができ、適切な処置を施すことが可能となり、コンピュータウィルスによるさらなる被害の拡大を未然に防止し得る。

【００６３】図５に、コンピュータ３がコンピュータ１に添付ファイルを含む電子メールを送信後、コンピュータ１がコンピュータ２にこの添付ファイルを含む電子メールをさらに送信し、それに対して、コンピュータ２がウィルス通知メールをワクチンソフトウェアとともに、コンピュータ１に対し送信した場合に、コンピュータ１において行われる処理のフローチャートを示す。

【００６４】図５に示すように、コンピュータ１において、コンピュータ２により送信された前述のウィルス通知メールがメイル受信手段１ｂにより受信されると、まず、受信した電子メールに添付されるワクチンソフトウェアを用いて、コンピュータウィルスが発見された添付ファイルのコンピュータウィルスを駆除する（ステップＳ１０）。

【００６５】そして、記憶装置５の添付ファイル情報デ

ータベース領域５ｂの検索を開始し（ステップＳ１１）、前記コンピュータウィルスが発見された添付ファイルのファイル名が登録されているか否かを調べる。その結果、登録されている場合（ステップＳ１２；ＹＥＳ）、送信者情報領域５ｃを参照し、当該添付ファイルを送信した送信者であるコンピュータ３の送信者情報を調べ、コンピュータ３に対し、発見したコンピュータの名称を含み、適合するワクチンソフトウェアを添付ファイルとするウィルス通知メールをメイル送信手段１ａにより送信し（ステップＳ１３）、処理を終了する。

【００６６】一方、コンピュータウィルスが発見された添付ファイルのファイル名が登録されていない場合（ステップＳ１２；ＮＯ）、ステップＳ１３の処理を行わず、処理を終了する。

【００６７】以上の処理により、コンピュータウィルスの発見できないまま、電子メールより感染したファイルを送信した場合でも、送信先においてコンピュータウィルスを発見されれば、そのウィルス情報と駆除プログラムが入手でき、データベースによりファイル受信履歴を調べてさらに元の送信者をたどってウィルス情報等を送信することができるので、複雑な伝搬経路を伝わり広がるコンピュータウィルスに対して、適切な処置を施すことが可能となる。

【００６８】なお、図４及び図５に示す処理においては、送信元のコンピュータに対するウィル検出情報、ワクチンソフトウェアなどの送信処理は、電子メールを用いたウィルス通知メールによる行うこととしたが、コンピュータの操作者の処理を介在させず、受信ファイルにウィルスが検出された場合、自動的に送信元のコンピュータに対し通知を行うこととしてもよい。

【００６９】また、上述した本発明に係るコンピュータシステムにおけるコンピュータウィルス対抗方法を処理するプログラムは、ネットワーク上のコンピュータにおいて読み取り可能なＣＤ－ＲＯＭ、フロッピィーディスク等の記録媒体に記録させることが可能である。そして、当該ＣＤ－ＲＯＭ等を用いてコンピュータにおいてコンピュータウィルス対抗プログラムを処理するプログラムをインストールし、実行することにより、本発明のコンピュータシステムが実現される。

【００７０】

【発明の効果】以上説明したように、請求項１に記載のコンピュータシステムによれば、ネットワーク上の他のコンピュータからファイルを受信する際、ファイル送信元とファイルのコンピュータウィルスを検出し、コンピュータウィルスが検出されると検出情報を送信元に送信するので、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識でき、コンピュータウィルスに対する適切な対策を施すことが可能となる。従って、自らコンピュータウィルスの検出ができないコンピュータからの再感染を防ぎ、被害の拡大の未然防止を図ることができる。

【００７１】請求項２に記載のコンピュータシステムによれば、ファイル付属情報を受信ファイルと関係付けて記憶し、受信ファイルにおいてコンピュータウィルスが検出されると、ファイル付属情報より送信元を調べ、送信元がわかるとコンピュータウィルスの検出情報を送信するようにしたので、ファイル受信時にコンピュータウィルスを検出できない場合、その後のコンピュータウィルス発見時にファイルの受信履歴を活用して、請求項１と同様の処理を行うことができる。従って、現在又は過去において伝搬したコンピュータウィルスに対する適切な処置を、処置可能となった時点で迅速に施すことができ、被害の拡大を最小限に抑えることができる。

【００７２】請求項３に記載のコンピュータシステムによれば、受信ファイルを、更に別のコンピュータに転送した後に、転送ファイルに関するコンピュータウィルスの検出情報を受信した場合、ファイル付属情報に送信元が記憶されていれば、この送信元に対しコンピュータウィルスの検出情報を更に送信するようにしたので、別のコンピュータにコンピュータウィルスに感染したファイルを転送してしまった場合でも、その後送信元のコンピュータにコンピュータウィルスの存在を知らしめることができ、コンピュータウィルスに対する適切な対策を施すことが可能となる。従って、ネットワーク上を複雑な伝搬経路を経てコンピュータウィルスが伝わる場合でも、その伝搬経路の元を次々と辿って適宜に処置することでき、被害が広範に渡って拡大するのを防止することができる。

【００７３】請求項４に記載のコンピュータシステムによれば、受信ファイルにコンピュータウィルスが検出されると、駆除ソフトウェアを送信元のコンピュータに対し送信するようにしたので、送信元のコンピュータは、コンピュータウィルスに感染していることを認識できることに加え、対策手段としての駆除ソフトウェアを併せて入手でき、速やかに適切な対策を施すことが可能となる。従って、各コンピュータにおいて駆除ソフトウェアが用意されているかどうかにかかわらず、迅速な処置を施すことができ、コンピュータウィルスを速やかに除去できる。

【００７４】請求項５に記載のコンピュータウィルス対抗プログラムによれば、ネットワーク上の他のコンピュータからファイルを受信する際、ファイル送信元とファイルのコンピュータウィルスを検出し、コンピュータウィルスが検出されると検出情報を送信元に送信するので、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識でき、コンピュータウィルスに対する適切な対策を施すことが可能となる。従って、自らコンピュータウィルスの検出ができないコンピュータからの再感染を防ぎ、被害の拡大の未然防止を図ることができる。

【００７５】請求項６に記載のコンピュータウィルス対抗プログラムによれば、ファイル付属情報を受信ファイルと関係付けて記憶し、受信ファイルにおいてコンピュータウィルスが検出されると、ファイル付属情報より送信元を調べ、送信元がわかるとコンピュータウィルスの検出情報を送信するようにしたので、ファイル受信時にコンピュータウィルスを検出できない場合、その後のコンピュータウィルス発見時にファイルの受信履歴を活用して、請求項１と同様の処理を行うことができる。従って、現在又は過去において伝搬したコンピュータウィルスに対する適切な処置を、処置可能となった時点で迅速に施すことができ、被害の拡大を最小限に抑えることができる。

【００７６】請求項７に記載のコンピュータウィルス対抗方法によれば、受信ファイルとファイル付属情報を、更に別のコンピュータに転送した後に、転送ファイルに関するコンピュータウィルスの検出情報を受信した場合、ファイル付属情報に送信元が記憶されていれば、この送信元に対しコンピュータウィルスの検出情報を更に送信するようにしたので、別のコンピュータにコンピュータウィルスに感染したファイルを転送してしまった場合でも、その後送信元のコンピュータにコンピュータウィルスの存在を知らしめることができ、コンピュータウィルスに対する適切な対策を施すことが可能となる。従って、ネットワーク上を複雑な伝搬経路を経てコンピュータウィルスが伝わる場合でも、その伝搬経路の元を次々と辿って適宜に処置することでき、被害が広範に渡って拡大するのを防止することができる。

【００７７】請求項８に記載のコンピュータウィルス対抗方法によれば、受信ファイルにコンピュータウィルスが検出されると、駆除ソフトウェアを送信元のコンピュータに対し送信するようにしたので、送信元のコンピュータは、コンピュータウィルスに感染していることを認識できることに加え、対策手段としての駆除ソフトウェアを併せて入手でき、速やかに適切な対策を施すことが可能となる。従って、各コンピュータにおいて駆除ソフトウェアが用意されているかどうかにかかわらず、迅速な処置を施すことができ、コンピュータウィルスを速やかに除去できる。

【００７８】請求項９に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、ネットワーク上の他のコンピュータからファイルを受信する際、ファイル送信元とファイルのコンピュータウィルスを検出し、コンピュータウィルスが検出されると検出情報を送信元に送信するので、送信元のコンピュータは、送信したファイルがコンピュータウィルスに感染していることを認識でき、コンピュータウィルスに対する適切な対策を施すことが可能となる。従って、自らコンピュータウィルスの検出ができないコンピュータからの再感染を防ぎ、被害の拡大の未然防止を図ることができる。

【００７９】請求項１０に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、ファイル付属情報を受信ファイルと関係付けて記憶し、受信ファイルにおいてコンピュータウィルスが検出されると、ファイル付属情報より送信元を調べ、送信元がわかるとコンピュータウィルスの検出情報を送信するようにしたので、ファイル受信時にコンピュータウィルスを検出できない場合、その後のコンピュータウィルス発見時にファイルの受信履歴を活用して、請求項１と同様の処理を行うことができる。従って、現在又は過去において伝搬したコンピュータウィルスに対する適切な処置を、処置可能となった時点で迅速に施すことができ、被害の拡大を最小限に抑えることができる。

【００８０】請求項１１に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、受信ファイルを、更に別のコンピュータに転送した後に、転送ファイルに関するコンピュータウィルスの検出情報を受信した場合、ファイル付属情報に送信元が記憶されていれば、この送信元に対しコンピュータウィルスの検出情報を更に送信するようにしたので、別のコンピュータにコンピュータウィルスに感染したファイルを転送してしまった場合でも、その後送信元のコンピュータにコンピュータウィルスの存在を知らしめることができ、コンピュータウィルスに対する適切な対策を施すことが可能となる。従って、ネットワーク上を複雑な伝搬経路を経てコンピュータウィルスが伝わる場合でも、その伝搬経路の元を次々と辿って適宜に処置することでき、被害が広範に渡って拡大するのを防止することができる。

【００８１】請求項１２に記載のコンピュータウィルス対抗プログラムが記録された記録媒体を読み取り実行するコンピュータによれば、受信ファイルにコンピュータウィルスが検出されると、駆除ソフトウェアを送信元のコンピュータに対し送信するようにしたので、送信元のコンピュータは、コンピュータウィルスに感染していることを認識できることに加え、対策手段としての駆除ソフトウェアを併せて入手でき、速やかに適切な対策を施すことが可能となる。従って、各コンピュータにおいて駆除ソフトウェアが用意されているかどうかにかかわらず、迅速な処置を施すことができ、コンピュータウィルスを速やかに除去できる。

【図面の簡単な説明】

【図１】本発明の実施形態における印刷システムの概略構成を説明する図である。

【図２】本発明の実施形態におけるコンピュータのハードウェア構成を示すブロック図である。

【図３】本発明の実施形態におけるコンピュータを機能の面から捉えて説明するためのブロック図である。

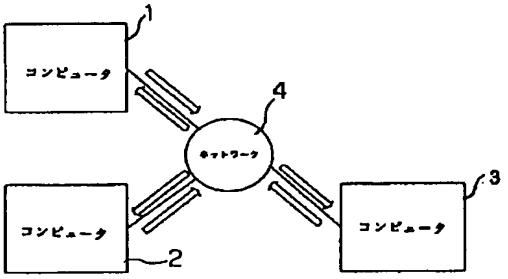
【図４】本発明の実施形態における電子メール受信時のコンピュータウィルスに対する対抗方法を説明するフローチャートである。

【図５】本発明の実施形態におけるウィルス通知メール受信時のコンピュータウィルスに対する対抗方法を説明するフローチャートである。

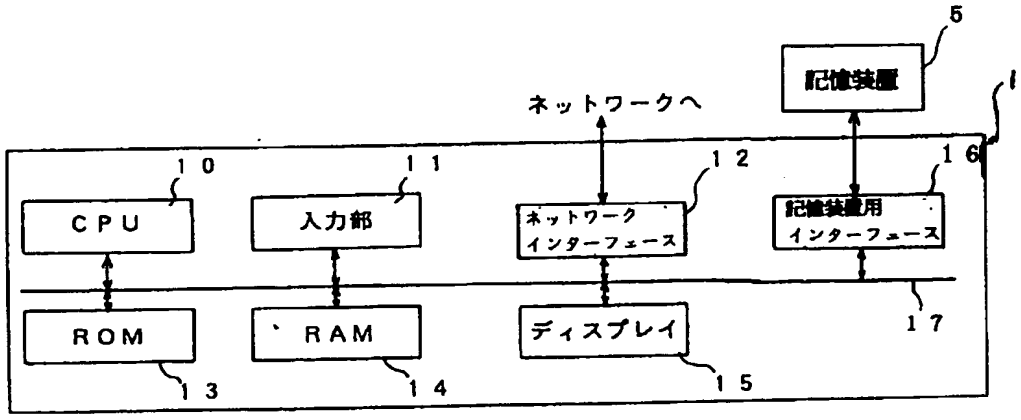
【符号の説明】

１、２、３…コンピュータ
１ａ…メイル送信手段
１ｂ…メイル受信手段
１ｃ…メイル送信者検出手段
１ｄ…ウィルス検出手段
１ｅ…ウィルス駆除手段
４…ネットワーク
５…記憶装置
５ａ…添付ファイル領域
５ｂ…添付ファイル情報データベース領域
５ｃ…送信者情報領域
１０…ＣＰＵ
１１…入力部
１２…ネットワークインターフェース
１３…ＲＯＭ
１４…ＲＡＭ
１５…ディスプレイ
１６…記憶装置用インターフェース
１７…バス

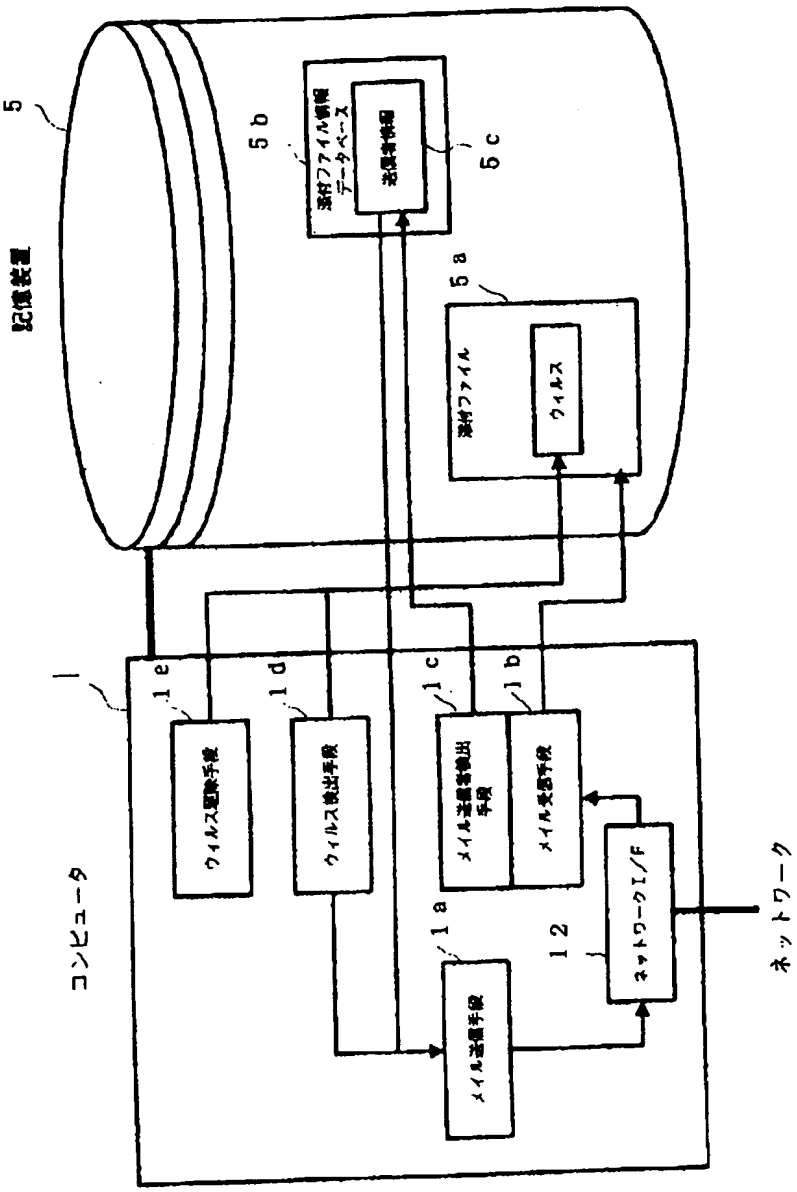
【図１】



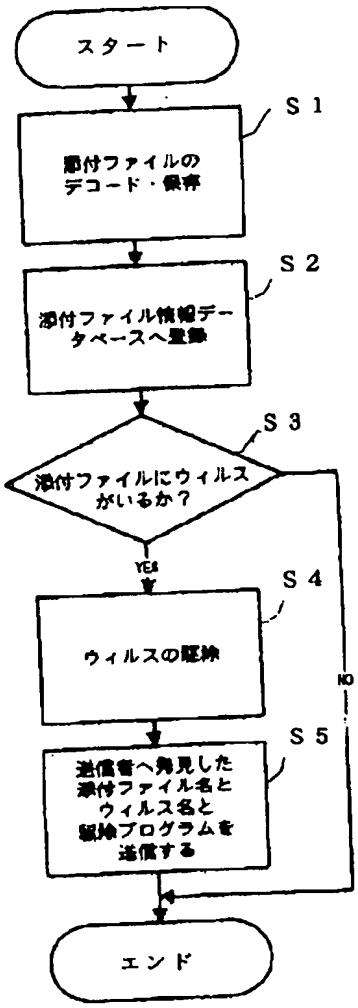
【図２】



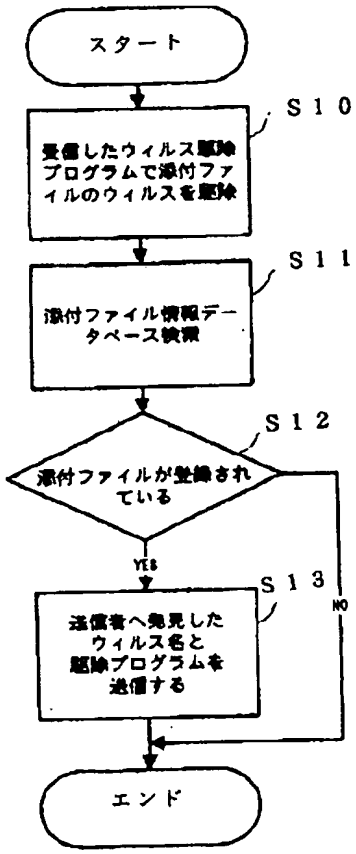
【図３】


5
記憶装置
5b
添付ファイル情報データベース
送信者情報
5c
5a
添付ファイル
ウィルス
1
コンピュータ
1e
ウィルス駆除手段
1d
ウィルス検出手段
1c
メイル送信者検出手段
1b
メイル受信手段
1a
メイル送信手段
12
ネットワークI/F
ネットワーク

【図４】


スタート
S１
添付ファイルのデコード・保存
S２
添付ファイル情報データベースへ登録
S３
添付ファイルにウィルスがいるか？
YES
NO
S４
ウィルスの駆除
S５
送信者へ発見した添付ファイル名とウィルス名と駆除プログラムを送信する
エンド

【図５】


スタート
S１０
受信したウィルス駆除プログラムで添付ファイルのウィルスを駆除
S１１
添付ファイル情報データベース検索
S１２
添付ファイルが登録されている
YES
NO
S１３
送信者へ発見したウィルス名と駆除プログラムを送信する
エンド